IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CRYSTAL BYRD and **BRIAN BYRD**, Individually, and on Behalf of all Similarly Situated Persons,	)	
Plaintiffs,	)	
vs.	)	Civil No. 11-101
AARON'S, INC., **ASPEN WAY ENTERPRISES, INC.**, d/b/a Aaron's Sales and Leasing, a franchisee of AARON'S, INC.; **JOHN DOES (1-100) AARON'S FRANCHISEES;** and **DESIGNERWARE, LLC**,	)	
Defendants.	)	

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Crystal and Brian Byrd, individually and on behalf of all similarly situated persons, by and through their undersigned attorneys allege the following upon information and belief (except for those allegations pertaining to Plaintiffs, which are based on personal knowledge) after due investigation by undersigned counsel.

NATURE OF THE ACTION

1. Plaintiffs, Crystal and Brian Byrd, bring this action on their own behalf and as a Class Action for the benefit of a class consisting of all customers of Aaron's, Inc. ("Aaron's") and its franchisees including Aspen Way Enterprises ("Aspen Way") and other John Doe franchisees (collectively hereafter referred to as the "Aaron's Defendants") who reside in the United States, who have purchased, leased, rented or rented to own ("RTO"), Aaron's computers and people who used said computers whose electronic communications and/or images were

intercepted, accessed, monitored and/or transmitted by a spying device or software without the customer's authorization (including software called "PC Rental Agent®" manufactured by co-defendant DesignerWare, LLC, ("DesignerWare")) wherever they may reside in the United States of America.

2. Plaintiffs and the Class seek injunctive relief and damages caused by Defendants' unlawful interception of electronic communications and images in violation of the Federal Wiretap Act as amended by the Electronic Communications Privacy Act (hereinafter referred to as the "Wiretap Act" or the "Electronic Communications Privacy Act"), and the Computer Fraud Abuse Act. ("CFAA").

3. Unbeknownst to Plaintiffs and the members of the Class, and without their authorization, Defendants have been spying on the activities of Plaintiffs and Class members through the use of the PC Rental Agent® device and/or similar Software and/or devices which were designed to, and in fact did, access, intercept, transmit, use and/or disclose electronic communications. These spying devices and/or spying software were installed and enabled surreptitiously without the consent of Plaintiffs or Class members.

THE PARTIES, JURISDICTION AND VENUE

4. Plaintiffs and the Class bring this action pursuant to §§ 2511, 2512 and 2520 of title 18 of the United States Code also known as the Electronic Communication Privacy Act ("ECPA") or Wiretap Act; and § 1030 of the Computer Fraud and Abuse Act ("CFAA").

5. This Court has original jurisdiction of Plaintiffs' and the Class' federal law claims pursuant to 28 U.S.C. §§ 1331 and 1337.

6. Plaintiff Crystal Byrd is a resident of Casper, Natrona County, Wyoming, and was a customer of Aaron's and/or Aspen Way, by virtue of her rental and purchase of a laptop computer from the Aaron's store located at 4050 Plaza Drive, Casper, Wyoming.

7. Plaintiff Brian Byrd is a resident of Casper, Natrona County, Wyoming, and was an authorized user of an Aaron's and or Aspen Way's computer.

8. Defendant DesignerWare, LLC, is a Pennsylvania limited liability corporation, with a principal place of business in North East, Pennsylvania. DesignerWare, LLC designed, manufactured, assembled, possessed, marketed, advertised and sold to the Aaron's Defendants the devices and/ or software (including PC Rental Agent®) which permitted the illegal and wrongful activity further described herein.

9. Defendant Aaron's is a Georgia corporation, with a principal place of business in Atlanta, Georgia, and has retail store locations through America, including Pennsylvania, and other states and territories of the United States. During the time relevant to this Complaint, Aaron's purchased, installed and/or used PC Rental Agent® and installed it on computers it offered for rent or sale without authorization from its customers. Through the use of PC Rental Agent® and technical support offered by DesignerWare in Pennsylvania, Aaron's purposely availed itself to the jurisdiction of the state of Pennsylvania.

10. Defendant Aspen Way Enterprises, Inc., d/b/a Aaron's Sales and Leasing is a franchisee of Aaron's, Inc., and is a Montana business which has retail stores in Wyoming and other states. During the time relevant to this Complaint, Aspen Way purchased, installed and/or used PC Rental Agent® and installed it on computers it offered for rent or sale without authorization from its customers. Through the use of PC Rental Agent® and technical support

offered by DesignerWare in Pennsylvania, Aspen Way purposely availed itself to the jurisdiction of the state of Pennsylvania.

11. The John Does Defendants are Aaron's franchisees who have purchased PC Rental Agent® and installed it on their computers for rent or purchase without authorization from their customers. Through the use of PC Rental Agent® and technical support offered by DesignerWare in Pennsylvania, the John Does purposely availed themselves to the jurisdiction of the state of Pennsylvania.[1]

12. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391 (b) and (c) as DesignerWare, LLC, the designer and distributor of PC Rental Agent® device and/or software, has its principal place of business is located in North East, Pennsylvania. Moreover, upon information and belief, DesignerWare receives, manages, stores, intercepts, discloses and transmits communications intercepted by PC Rental Agent® and/or Software for the Aaron's Defendants in this district.

13. Venue is proper in this district because the Aaron's Defendants received, managed, accessed, intercepted and transmitted communications collected in this district through the use of the PC Rental Agent® device and/or software intentionally installed on their rental computers throughout the country (including the computer rented, owned and used by class plaintiffs Crystal and Brian Byrd).

14. In connection with the acts and conduct complained of below, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including the internet, or made such use possible.

---

[1] Defendant DesignerWare – through its counsel – has declined plaintiff's request for identification of Franchisees which have "activated" the Detective Mode of PC Rental Agent, making an amendment to identify these Doe defendants impossible at this time. Plaintiffs will seek leave of Court to make said amendment should DesignerWare disclose the identities of these Franchisees.

CLASS ACTION ALLEGATIONS

15. Plaintiffs Crystal and Brian Byrd bring this action on behalf of themselves and a Class of all other persons similarly situated pursuant to Fed. R. Civ. P. 23 as defined as follows:

> All customers of the Aaron's Defendants who reside in the United States, who have purchased, leased, rented or rented to own, Aaron's computers and people who used said computers whose electronic communications and/or images were intercepted, accessed, monitored and/or transmitted by Defendants via PC Rental Agent® or other devices or software without the customer's authorization.

16. Specifically excluded from the Class are the Defendants themselves, any subsidiary of any of the Defendants, any family members of the Defendants who are such customers, all employees and directors of Defendants or any subsidiary, and their legal representatives.

17. The Class is so numerous that joinder of all members is impracticable. The Customers of the Aaron's Defendants who have similarly purchased, leased, rented or rented to own ("RTO") such computers are estimated to be greater than two thousand individuals and entities.

18. Plaintiffs' claims are typical of the Class, as plaintiffs and all other Class members were injured in exactly the same way – by the unauthorized collection, interception and/or transmission of electronic communications through PC Rental Agent® (or similar devices or software) installed on their Aaron's RTO computer.

19. Plaintiffs will fairly and adequately represent the interests of the Class and have retained counsel competent and experienced in Class Action litigation.

20. Plaintiffs have no interests that are contrary to or in conflict with those of the Class.

21. A Class Action is superior to other available methods for the fair and efficient adjudication of this controversy under the acts described below. Given the nature of these claims, the expense and burden of individual litigation make it virtually impossible for the Class members individually to seek redress for the unlawful conduct alleged.

22. Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a Class Action.

23. Common questions of law and fact exist as to all members of the Class and predominate over any questions effecting solely individual members of the Class. Among the questions of law and fact, common to the Class:

a. Whether Defendants' acts as alleged herein violated the ECPA and/or CFAA.

b. Whether Defendants participated in and pursued the concerted action or common course of conduct complained of;

c. Whether Plaintiffs and members of the Class are entitled to statutory and punitive damages pursuant to the ECPA and/or CFAA; and

d. Whether Plaintiffs and members of the Class are entitled to injunctive relief.

24. Plaintiffs bring this action under Rule 23(b)(2) because Defendants have acted or refused to act on grounds generally applicable to all members of the Class, thereby making final injunctive relief concerning the Class as a whole appropriate. In the absence of appropriate injunctive relieve, Defendants will continue to unlawfully violate the rights of Plaintiffs and the

members of the Class by illegally intercepting, accessing and/or transmitting personal and private information and communications contrary to federal law. Defendants' uniform conduct towards Plaintiffs and the other members of the Class makes certification under Rules 23 (b)(2) appropriate.

25. Plaintiffs also bring this action under Rule 23(b)(3) because common questions of law and fact identified in paragraph 23 above predominate over questions of law and fact affecting individual members of the Class. Indeed, the predominate issues in this class are whether Defendants are violating and have violated the law by the unauthorized, inappropriate and undisclosed remote interception and transmission of communications and information secretly obtained by computers rented, leased and/or sold to said Class members, and in the intentional unauthorized interception and use of electronic and computer communications and information, including "screen shots," photographs and information (including keystrokes) relating to internet usage. Certification under Rule 23(b)(3) is appropriate because:

a. by virtue of the secret nature of the spying device and software described in this complaint, individual class members may not be aware that they have been wronged and are thus unable to prosecute individual claims;

b. concentration of the litigation concerning this matter in this Court is desirable;

c. the claims of the representative Plaintiffs are typical of the claims of the members of the purported class;

d. a failure of justice will result from the absence of a class action; and

e. the difficulties likely to be encountered in the management of this class action are not great.

SUBSTANTIVE ALLEGATIONS

26. Since 2007, the Aaron's Defendants have secretly installed a spying device and/or software on Aaron's RTO computers. This device and/or software, including PC Rental Agent®, permitted the Aaron's Defendants to remotely and surreptitiously access, monitor, intercept, and/or transmit electronic communications, including, but not limited to, images of monitors or screens ("screen shots"), keystrokes, and images captured by the computers' respective cameras ("webcams").

27. PC Rental Agent® and other similar devices and software as referenced in this Complaint, make possible such illegal, surreptitious, and unauthorized remote interception of protected communications.

28. PC Rental Agent® is manufactured, assembled, advertised and sold to the Aaron's Defendants by DesignerWare for the primary purpose of allowing the Aaron's Defendants to remotely track, access, monitor, monitor and/or transmit electronic communications on Aaron's RTO computers.

29. PC Rental Agent® is a device and/or software that is manufactured, advertised to be and is, in fact, invisible or undetectable to customers and to other end users of Aaron's RTO computers.

30. Upon information and belief, PC Rental Agent® cannot be uninstalled or easily detected.

31. PC Rental Agent® allows the Aaron's Defendants, DesignerWare and their agents to surreptitiously monitor, intercept and collect Plaintiffs' electronic communications from anywhere in the world.

32. It has been the practice and policy of the Aaron's Defendants to conceal from their customers their ability to remotely access, intercept and monitor customers' private, personal electronic communications, information, screen shots, keystrokes or images captured on webcams and to further disclose to consumers exactly the kinds of private information and images that can be and were routinely collected, transmitted and stored.

33. The Aaron's Defendants' sales, rental or lease agreements neither seeks permission from nor discloses to RTO customers the presence of PC Rental Agent® or its ability to monitor and intercept communications and other data from Aaron's RTO computers.

34. On July 30, 2010, Plaintiff Crystal Byrd entered into an Aaron's RTO lease agreement for a "Dell Inspiron 14" laptop computer. The Byrd lease agreement provided that Crystal Byrd would pay three separate installments by November 15, 2010 for the purchase of said computer. [Ex. 1, "Consumer Lease Agreement and Federal Consumer Leasing Act Disclosures" ("Lease Agreement")].

35. It was the common practice for Aspen Way to invoice and accept payment from its customers via the internet.

36. The Byrd lease agreement did not disclose that the Aaron's Defendants had installed a device which could monitor the Byrds and intercept their private communications.

37. The Byrd's timely paid off the lease "in full," according to the lease agreement terms, by October 1, 2010.

38. On or about December 22, 2010, Brian Byrd was using the aforementioned computer, playing poker on the internet, when – unbeknownst to him and without his permission or authority – a photograph of him and a screenshot of his computer screen, showing the internet page with which he was communicating, and from which he was receiving communications, as

well as the keystrokes he was entering into the computer while communicating with the online internet site, were captured and sent from his computer to the Designerware server in Pennsylvania, which, in turn, transmitted said photograph, screenshot and keystrokes to the Casper, Wyoming Aaron's (Aspenway) store.

39. On or about the 22nd day of December, 2010, Christopher Mendoza, the store manager for the Aaron's store in Casper, Wyoming, went to the home of class representatives Brian and Crystal Byrd. At that time, Mendoza incorrectly claimed that the Byrds were in default on their lease agreement and demanded that the Byrd computer be returned to Aaron's. To further support his attempts to collect the Byrd computer, Mendoza informed co-plaintiff Brian Byrd that he had obtained a photograph of Brian Byrd while using the internet on his computer – and Mendoza showed Byrd the photograph and screenshot which had been taken and intercepted remotely using the PC Rental Agent® as referenced in the preceding paragraph. When Brian Byrd demanded that Mendoza explain how Mendoza had obtained an unauthorized photograph, Mendoza responded that he was not supposed to disclose that Aaron's had the photograph.

40. Byrd told Mendoza that, contrary to Mendoza's claim, the computer had been paid "in full" and advised that Mendoza needed to leave, at which point Mendoza left the Byrd residence.

41. Following his encounter with Mendoza, co-plaintiff Brian Byrd contacted law enforcement to report the incident. Law enforcement responded to the Byrd residence and commenced an investigation.

42. Upon information and belief, the law enforcement investigation determined that on or about the 22nd of December, Mendoza was directed by his supervisor, Sian Baker, to

retrieve Crystal Byrd's computer because the Byrds were allegedly (but incorrectly) in default of their RTO lease agreement.

43. Upon information and belief, Baker provided Mendoza the photograph of Brian Byrd taken by the PC Rental Agent® device; the photograph that Mendoza later showed to Brian and Crystal Byrd, and directed Mendoza to repossess the computer.

44. Upon information and belief, the law enforcement investigation further determined that one or more of the Aaron's Defendants routinely installed the PC Rental Agent® device and/or software on all Aaron's RTO computers, and that this device and/or software permitted Defendants to remotely gather, intercept, transmit and store private electronic information and communications from RTO customers, including but not limited to photographs, screen shots and keystrokes.

45. Upon information and belief, the law enforcement investigation further determined that neither Baker nor Mendoza had access or authority to change PC Rental Agent® settings on the Byrd computer. In fact, it is understood that the authority to change settings on the PC Rental Agent® installed on RTO computers resided with the regional managers of the Aaron's Defendants.

46. Upon information and belief, the law enforcement investigation further determined that the Aaron's Defendants purchased the spying device called PC Rental Agent® from co-defendant DesignerWare.

47. Upon information and belief, Ashton Kelly, an agent or employee of DesignerWare, was interviewed by law enforcement and he confirmed that the PC Rental Agent® permitted (and continued to permit) the Aaron's Defendants to gather, transmit and store

screen shot images, keystrokes and photographs taken via the webcam without the customer's knowledge or consent

48. Upon information and belief, the law enforcement investigation determined that the communications and other data captured by the PC Rental Agent® was transmitted from Aaron's RTO computers to a central server operated by DesignerWare located in Pennsylvania where the data was then made available to the Aaron's Defendants throughout the country

49. Upon information and belief, Ashton Kelly further advised law enforcement that the photographs are taken remotely via the webcam through "prompting," which occurs when the customer receives a "pop-up" box on his computer screen which states that the customer's windows system registry, or part of the windows software, needs to be registered.

50. The "pop-up" box described in the previous paragraph further requires the Aarons RTO customer (or any authorized user) to enter his or her name, address and telephone number, after which they are given access to the computer. At the time the user enters the information, the PC Rental Agent® causes the webcam to take, transmit and store an unauthorized photograph and other data of the user entering the information. Neither the "pop-up" box nor any other statement from any Defendant (including the Rental Agreement) notified or advised the Byrds (or any end user) that private electronic communications were being intercepted and/or monitored.

51. While law enforcement was conducting its investigation at the Casper Aaron's store, it is further believed that a law enforcement officer observed an unauthorized photograph of another Aaron's customer, and was told that Aaron's regularly received Emails from DesignerWare with unauthorized photographs and other communications taken of customers and authorized users through the use of the PC Rental Agent®.

52. Aaron's, Inc. sponsors Annual Manager's Meetings, the purpose of which is to provide information to the entire Aaron's franchise, including Aaron's corporate stores and Aaron's franchisees. Generally, Annual Managers Meetings are attended by Aaron's General Managers, Regional Managers, and owners.

53. On April 10-12, 2007, Aaron's, Inc. held its annual National Managers Meeting at the Gaylord Texan Resort and Convention Center in Grapevine, Texas. Over 2,000 managers, executives and home office personnel attended the event.

54. At that 2007 meeting, Aaron's Director of Western Franchise Operations introduced the attendees to PC Rental Agent®.

55. Since that meeting, more than 100 franchisees have purchased and installed PC Rental Agent® on their RTO computers.

56. It is upon information and belief that defendants' intercept data from members of the class that include personal and/or private information, *i.e.* on-line banking communications, passwords, notes to physicians, etc. Defendants' do not filter sensitive or private data when they illegally intercept information from the members of the class.

CAUSES OF ACTION

COUNT I
(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511)

57. Plaintiffs repeat and re-allege each and every allegation above as if fully set forth herein.

58. Defendants, either directly or by aiding, abetting and/or conspiring to do so, have intentionally intercepted and/or procured to be intercepted Plaintiffs' and Class members' electronic communications without Plaintiffs' or the Class members' knowledge, authorization, or consent in violation of 18 U.S.C. § 2511.

59. Defendants, either directly or by aiding, abetting and/or conspiring to do so, have also intentionally used and/or procured to be used a devise to intercept the above-referenced electronic communications.

60. Defendants, either directly or by aiding, abetting and/or conspiring to do so, have intentionally disclosed to another person, and/or used the contents of the above-referenced electronic communications.

61. An "electronic communication" is defined in § 2510(12) as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.

62. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally, collecting, gathering intercepting, endeavoring to intercept, transmit, procure, store any other person to intercept or endeavor to intercept Plaintiffs' and Class members' electronic communications.

63. Defendants violated 18 U.S.C. § 2511(1)(c) by intentionally collecting, transmitting, storing and disclosing, or endeavoring to disclose, to any other person, the contents of Plaintiffs and Class members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' and class members electronic communications.

64. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using or endeavoring to use, the contents of Plaintiffs' and class members electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' electronic communications.

65. Neither Plaintiffs nor class members authorized or consented to Defendants' interception of electronic communications.

66. Section 2520 of the ECPA provides for a private cause of action and allows for declaratory and equitable relief as appropriate and statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, and reasonable attorney's fees and costs.

67. Unless restrained and enjoined, Defendants have been and will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiffs and Class members to remedies including injunctive relief as provided by 18 U.S.C. § 2510.

COUNT II
(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2512)

68. Plaintiffs, on behalf of themselves and the Class, hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

69. Defendants, either directly or by aiding, abetting and/or conspiring to do so, have intentionally manufactured, assembled, possessed, sold, and/or advertised a device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications and that such device or advertisement relating to such device has been or will be sent through the mail or transported in interstate in violation of 18 U.S.C. § 2512.

70. An "electronic communication" is defined in § 2510(12) as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.

71. Defendants violated 18 U.S.C. § 2512(1)(a) by intentionally sending and/or carrying through the mail or interstate commerce a device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications.

72. Defendants violated 18 U.S.C. § 2512(1)(b) by intentionally manufacturing, assembling, possessing and/or selling a device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate commerce.

73. Defendants violated 18 U.S.C. § 2512(1)(c)(i) by intentionally advertising a device, knowing the content of the advertisement and knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications, knowing the content of the advertisement and having reason to know that such advertisement will be sent through the mail or transported in interstate commerce.

74. Defendants violated 18 U.S.C. § 2512(1)(c)(ii) by intentionally advertising a device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of electronic communications, knowing the content of the advertisement and having reason to know that such advertisement will be sent through the mail or transported in interstate commerce.

75. Section 2520 of the ECPA provides for a private cause of action and allows for declaratory and equitable relief as appropriate and statutory damages of the greater of $10,000 or

$100 a day for each day of violation, actual and punitive damages, and reasonable attorney's fees and costs.

76. Unless restrained and enjoined, Defendants have been and will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiffs and Class members to remedies including injunctive relief as provided by 18 U.S.C. § 2510.

COUNT III

(Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, et seq.)

77. Plaintiffs, on behalf of themselves and the Class, hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

78. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA") as amended, makes it unlawful to intentionally access a protected computer or communication without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of 18 U.S.C. § 1030(a)(2)(C).

79. Defendants violated 18 U.S.C. § 1030 by intentionally accessing Plaintiffs' and Class members' computers without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

80. The CFAA 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA.

81. Plaintiffs' computer is a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

82. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

83. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs' and Class members' protected computers without authorization, and as a result of such conduct, recklessly caused damage to Plaintiffs' and Class members computers by impairing the integrity of data and/or system and/or information.

84. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally accessing Plaintiffs' and Class members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiffs and Class members.

85. Plaintiffs and Class members suffered damage by reason of these violations, as defined in 18 U.S.C. § 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

86. Plaintiffs and Class members suffered damage by reason of these violations, as defined in 18 U.S.C. § 1030(e)(8), by the "reasonable costs . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

87. Plaintiffs and Class members suffered damage by reason of these violations, including, without limitation, violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record.

88. As a result of these takings, Defendants' conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages. PC Rental Agent is a "rootkit" and has directly affected the computer's ability to protect against viruses. Furthermore, PC Rental Agent has caused real and direct harm to data on the computer totaling in the aggregate more than $5,000.

89. Plaintiffs and Class members have additionally suffered loss by reason of these violations, including, without limitation, the right of privacy.

90. Defendants' unlawful access to Plaintiffs' and Class members' computers and electronic communications has caused Plaintiffs and Class Members irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts.

91. Plaintiffs and Class members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff and class members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

DEMAND FOR JURY TRIAL

Plaintiffs and the members of the Class hereby demand a trial by jury on all issues for which a right to jury trial exists.

LEVIN, FISHBEIN, SEDRAN & BERMAN

/s/ Daniel C. Levin
Frederick S. Longer
Bar No. PA 46653
flonger@lfsblaw.com
Arnold Levin
Bar No. PA 02280
alevin@lfsblaw.com
Daniel L. Levin
Bar No. PA 80013
dlevin@lfsblaw.com
510 Walnut Street, Suite 500
Philadelphia, Pennsylvania 19106-3697
Phone: 877-882-1011
Fax: 215-592-4663

JAMIESON & ROBINSON, LLC
John H. Robinson
Bar No. WSB 6-2828
robinsn@vcn.com
214 S. Grant Street
Casper, WY 82601
Phone: 307-235-3575
Fax: 307-307-577-9435

THE SPENCE LAWFIRM
G. Bryan Ulmer, III
ulmer@spencelawyers.com
Bar No. WY 6-2943
Mel C. Orchard, III
Bar No. WY 5-2984
orchard@spencelawyers.com
R. Daniel Fleck
Bar No. WY 6-2668
fleck@spencelawyers.com
PO Box 548 • 15 South Jackson Street
Jackson, Wyoming 83001
Phone: 307-733-7290
Fax: 307-733-5248

HERMAN GEREL LLP
Christopher V. Tisi
Bar No. DC 412839; MD 04286
cvtisi@aol.com
2000 L Street, NW Suite 400
Washington, D.C., 20036
Phone 202-783-6400
Fax: 202-416-6392

Michelle A. Parfitt
Bar No. VA 33650; DC 358592
mparf@aol.com
James F. Green
Bar No. VA 24915; DC 214965; MD 208980
jgreen@ashcraftlaw.com
4900 Seminary Road, Suite 650
Alexandria, Virginia 22311
Phone: 703-931-5500
Fax: 703- 820-0630

Maury A. Herman
Bar No. LA 006815
mherman@hhkc.com
Leonard A. Davis
Bar No. LA 14190
ldavis@hhkc.com
820 O'Keefe Avenue
New Orleans, LA 70113
Phone: 504-581-4892
Fax: 504-561-6024

Andrea S. Hirsch
Bar No. GA 666557
ahirsch@hermangerel.com
230 Peachtree Street, Suite 2260
Atlanta, GA 30303
Telephone: 404-880-9500
Fax: 404-880-9605

CERTIFICATE OF SERVICE

I, Daniel C. Levin, certify that a copy of the foregoing, FIRST AMENDED CLASS ACTION COMPLAINT was served via the Court's electronic notification system to all counsel of record on the 27th day of July, 2011.

/s/ Daniel C. Levin
Daniel C. Levin
Attorney for Plaintiffs